Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol. 14, Issue 14s (2025)
https://www.jneonatalsurg.com

OPEN ACCESS

Transformative Impact of Blockchain and Iot Integration in Healthcare

Nadiah Jaffreen Shaik[1], Dr. Tatavarthy Santhisri[2]

[1] Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation Guntur, India
Email ID: nadiahjaffreen@gmail.com

[2]Department of Computer Science and Engineering Koneru Lakshmaiah Education Foundation Guntur, India
Email ID: santhisri@kluniversity.in

Cite this paper as: Nadiah Jaffreen Shaik, Dr. Tatavarthy Santhisri, (2025) Transformative Impact of Blockchain and Iot Integration in Healthcare. *Journal of Neonatal Surgery*, 14 (14s), 340-348

ABSTRACT

Blockchain and IoT are transforming healthcare by enhancing data interchange, patient data security, and operational efficiency. Blockchain's decentralized ledger system protects medical data, lowers errors, and improves integrity. It increases healthcare data access transparency, accountability, and flexibility. Internet of Medical Things (IoMT) devices use blockchain authentication for secure health monitoring and healthcare operations. Cloud and fog computing are improving staff satisfaction and patient safety by storing and analyzing IoT data. Global e-health policies and regulations are essential for healthcare IoT and cloud computing development. Addressing privacy and security problems requires industry-specific security frameworks. Healthcare's IoT problems and potential are determining its future. This abstract explores the security and operational concerns of blockchain and IoT integration in healthcare and its transformational potential..

Keywords: *Blockchain, Internet of Things (IoT), Internet of Medical Things (IoMT), Healthcare, Data Security, Decentralized Ledger, Operational Efficiency, Patient Data, Cloud Computing, Fog Computing, Health Monitoring, E-health Policies, Data Privacy, Security Frameworks, Medical Data Integrity, Transparency, Accountability, Healthcare Innovation, Digital Health, Healthcare Regulations.*

1. INTRODUCTION

The convergence of blockchain technology and the Internet of Things (IoT) is fundamentally transforming the healthcare sector through a revaluation of data utilization, security, and exchange. The integrity and security of patient information are guaranteed by the decentralized ledger of Blockchain, whereas the network of interconnected devices of IoT facilitates the smooth exchange of data. These technologies are collectively improving the efficacy, effectiveness, and security of healthcare operations. Blockchain technology facilitates the exchange of data among medical entities, including pharmaceutical companies and institutions, in a secure and transparent manner. This secure exchange enhances data precision and reduces errors, resulting in improved patient outcomes. Additionally, the decentralized nature of blockchain ensures the confidentiality of patient information and prevents data tampering. A noteworthy implementation of blockchain technology within the healthcare sector is the authentication of Internet of Medical Things (IoMT) devices, which are integral to individualized health monitoring. Smart contracts based on the blockchain provide scalable authentication schemes that increase the authenticity of devices, decrease the likelihood of counterfeit devices, and ensure private information and secure updates. Fog computing and cloud computing have significantly improved patient safety and staff satisfaction, thereby transforming healthcare operations. The enormous quantities of patient data that are, nevertheless, at risk from the integration of IoT and cloud computing give rise to privacy and security concerns. To mitigate these risks, industry-specific security frameworks and a comprehensive comprehension of the emerging trends and challenges in IoT for healthcare are essential.

Related Work

The healthcare business is interested in blockchain and IoT convergence because it could improve data security, operational efficiency, and data interchange. Many studies have examined how these technologies affect healthcare processes. Blockchain's decentralized and immutable ledger technology improves data sharing and security, according to studies. Blockchain can securely store and manage patient data, making data interchange between hospitals, laboratories, pharmaceutical companies, and healthcare providers easier. Medical data is more accurate and reliable and centralized system errors are reduced by this secure data sharing that improves healthcare transparency and accountability. Technology's capacity to avoid data tampering and ensure data integrity is essential for accurate patient record analysis and educated healthcare decisions.

Decentralized data security decreases vulnerabilities and improves patient confidentiality, which is crucial in healthcare. Blockchain verification of IoMT devices is a major research field. The expanding use of IoMT devices for personalized

health monitoring and intelligent healthcare services requires a cyberattack-resistant authentication solution. Blockchain-based smart contracts allow scalable authentication for IoMT devices, eliminating counterfeit devices and assuring secure firmware updates, privacy, anonymity, and secrecy. According to research, cloud and fog computing have been used in healthcare due to IoT growth. Studies reveal that these technologies have transformed healthcare operations, improving staff satisfaction, patient safety, and productivity. Researchers have also explored how global e- health rules and regulations affect healthcare IoT and cloud computing sustainability. Healthcare data is delicate; thus, privacy and security are crucial. Industry-specific security frameworks have been evaluated for their ability to mitigate security risks, focusing on common threats and attacks. Studies on developing trends, possibilities, and problems have shed light on the future of IoT in healthcare and suggested additional study. This experiment shows how blockchain and IoT can transform healthcare. These technologies can boost healthcare innovation and outcomes by solving data security, operational efficiency, and authentication issues.

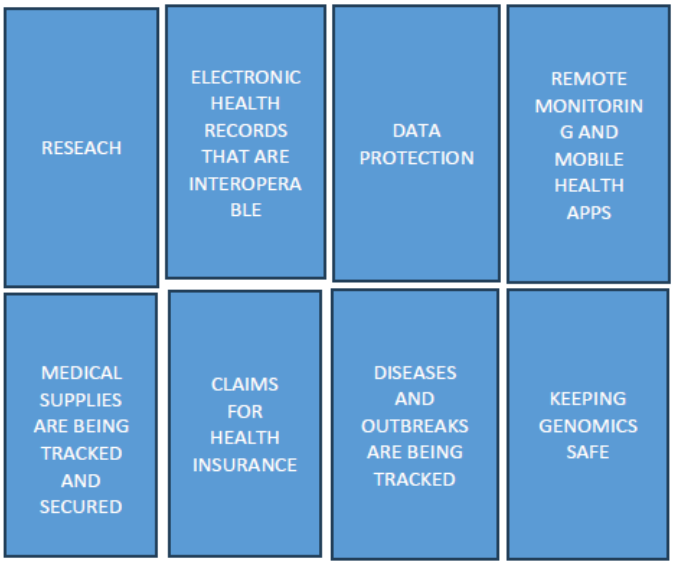
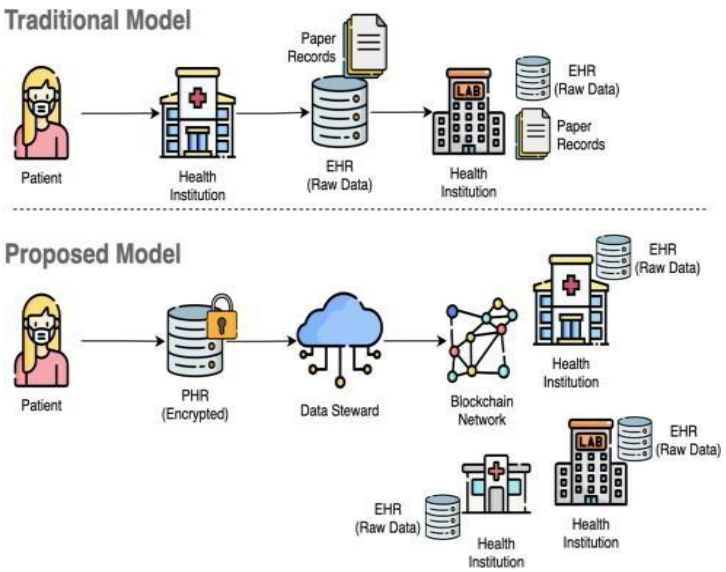


Figure 1: Blockchain in Healthcare

Due to the exponential growth in the number of human and machine-type devices, the next 6G wireless networks. Network densification is required, including end device (ED) densification and base station (BS) densification. The strategies have been successful in the past, but not effective in the new more densely populated network. This article analyses the BS and ED density characteristics of a dense network, and then it introduces new challenges and potential critical technologies.

Methodology

Figure 2: Traditional Model vs Proposed Model



a. Define the Scope and Objectives

- Identify key stakeholders in healthcare, including hospitals, laboratories, pharmaceutical companies, healthcare providers, and regulatory bodies.
- Define the primary objectives for using blockchain and IoT, such as secure data exchange, data integrity, operational efficiency, and improved patient care.

b. Implement Blockchain Infrastructure

- Choose an appropriate block chain platform (e.g., Ethereum, Hyperledger) that supports health care use cases.
- Establish a decentralized and immutable ledger system for healthcare data.
- Implement consortium or permissioned blockchain architectures to ensure controlled access and compliance with healthcare regulations (e.g., HIPAA, GDPR).

c. Integrate IoT Devices

- Identify critical IoT devices and sensors used in healthcare for personalized monitoring and intelligent healthcare services.
- Develop a scalable authentication scheme for Internet of Medical Things (IoMT) devices using blockchain-based smart contracts.
- Implement secure protocols for IoT device communication to prevent cyberattacks and unauthorized access.

d. Secure Data Exchange and Storage

- Ensure secure data exchange among stakeholders, using blockchain technology to improve precision and dependability of medical data transmission.
- Implement encryption techniques for data stored on block chain, ensuring confidentiality and data integrity.
- Design secure data storage mechanisms that are resilient against data tampering and unauthorized modifications.

e. Manage Cloud and Fog Computing Resources

- Integrate cloud computing and fog computing for scalable data storage and analysis.
- Design robust platforms to manage large-scale IoT data in healthcare environments. Leverage cloud/fog computing to improve operational efficiency and patient outcomes.

f. Address Privacy and Security Concerns

- Conduct regular security assessments and audits to identify potential vulnerabilities.
- Evaluate industry-specific security frameworks to ensure compliance with healthcare regulations and standards.
- Develop security policies and procedures to address emerging threats and protect patient data.

g. Implement a Monitoring and Alert System

- Set up real-time monitoring of blockchain and IoT networks to detect anomalies and security breaches. Implement automated alert systems to respond to potential threats promptly.
- Use blockchain's transparency to trace data transactions and investigate security incidents.

h. Develop e-Health Policies and Regulations

- Collaborate with global regulatory bodies to develop and update e-health policies that promote the sustainable development of IoT and cloud computing in health care.
- Ensure policies address privacy, security, and data protection in IoT-based healthcare applications.

i. Measure and Improve Healthcare Outcomes

- Establish metrics to assess the impact of blockchain and IoT integration on healthcare outcomes.
- Gather feedback from stakeholders to identify areas for improvement.

- Implement continuous improvement practices to enhance data exchange, security, and operational efficiency.

j. Plan for Future Trends and Challenges

- Identify emerging trends and challenges in blockchain and IoT technology.
- Develop strategic plans to address future risks and opportunities in healthcare.
- Foster innovation and research to keep pace with technological advancements and ensure long-term sustainability.

This algorithm provides a high-level overview of the integration and management of blockchain and IoT in healthcare while considering key factors such as security, operational efficiency, and regulatory compliance.

2. LITERATURE REVIEW

Blockchain technology and the Internet of Things (IoT) are integrating in a manner that is transforming the healthcare industry by facilitating improvements in data exchange, patient data security, and operational efficiency.

The decentralized and immutable ledger system of block chain improves the integrity and reliability of healthcare data, whereas the Internet of Things enables the interconnection of intelligent devices and sensors, thereby facilitating the exchange of data in a seamless manner.

Blockchain is gaining popularity due to its properties like decentralization, transparency, and identity management. It is widely integrated with technologies like IoT and cloud. It is implemented in areas like agriculture, logistics, finance, and quality checking. Precision agriculture/Internet of Agricultural Things (IoAT) uses block chain technology to identify the customer and cultivator productivity, product value, logistic management, dynamic prices, and churn rates related to the former's product. The predictive analysis algorithm for IoAT is developed to integrate data, identify malicious activity, and real-time data analysis between customers and formers in precision agriculture.

Blockchain technology is of the utmost importance when it comes to ensuring the secure exchange of patient information between pharmaceutical companies, healthcare providers, hospitals, laboratories, and labs. This secure data exchange improves the precision and dependability of medical data transmission while reducing errors. Moreover, block chain technology improves the transparency, security, and integrity of medical data, which is critical for the analysis of patient records and the formulation of well-informed judgments. In healthcare, block chain technology ensures data integrity, safeguards against data tampering, and provides secure data storage. In addition to providing authentication, connectivity, accountability, and flexibility, technology facilitates data access. Decentralized data security is a feature of blockchain technology that effectively reduces security vulnerabilities in healthcare environments, particularly those that prioritize the confidentiality of patient information. Its ability to safeguard data independently of a central authority is a significant factor in its advancement within the healthcare industry. An essential implementation of blockchain technology in the healthcare sector is the verification of Internet of Medical Things (IoMT) devices, which are vital for intelligent healthcare services and personalized health monitoring. Traditional centralized systems are susceptible to cyber-attacks; therefore, smart contracts based on the blockchain are an appealing alternative. Using blockchain technology, a scalable authentication scheme for IoMT devices ensures authenticity, reduces the risk of counterfeit devices, and ensures secure firmware updates, privacy, anonymity, and confidentiality. Cloud computing and fog computing have been implemented in healthcare because of the demand for robust platforms for data storage and analysis, which has been fueled by the exponential expansion of IoT technology. The implementation of these technologies has revolutionized healthcare operations, resulting in increased levels of staff contentment, patient protection, and overall productivity. The sustainable development of IoT and cloud computing in healthcare is influenced by global e- health policies and regulations. The integration of IoT and cloud computing streamlines data exchange and improves healthcare outcomes. It is of the utmost importance to tackle privacy and security concerns in Internet of Things (IoT) healthcare applications, given the substantial risks that patient data is exposed to from a multitude of threats and attack types. The effectiveness of industry-specific security frameworks in mitigating security risks is assessed, whereas predictions and challenges regarding the future of the Internet of Things in healthcare provide valuable insights.

k. Blockchain Applications in Healthcare

The passage mentions key applications of block chain technology in healthcare, highlighting its role in reducing fraud during clinical trials and enhancing data efficiency. These applications underscore the flexibility of blockchain and its capacity to address diverse healthcare challenges. Among these applications, some notable examples include

- Secure Data Storage

Blockchain provides a robust storage system, preventing unauthorized access and tampering.

- IoMT Device Authentication

A scalable authentication scheme for IoMT devices based on smart contracts has been proposed. This scheme leverages blockchain's secure and decentralized characteristics to ensure device authenticity and mitigate DDoS attacks.

- Secure Firmware Updates: The use of a consortium blockchain architecture guarantees confidentiality, anonymity, and privacy while protecting against counterfeit devices that utilize physical unclonable function (PUF) technology.

The scalability and security of blockchain-based systems make them attractive for healthcare applications, where patient safety and data privacy are paramount. The proposed IoMT authentication scheme implemented on the Ethereum platform demonstrates the practicality of using blockchain to enhance security in healthcare.

l. IoT and Cloud Computing in Healthcare:

Beyond blockchain, the exponential growth of the Internet of Things (IoT) has facilitated the interconnection of numerous intelligent devices and sensors, creating a seamless conduit for data exchange. In healthcare, this advancement has sparked interest from government agencies, researchers, and industry stakeholders. The integration of IoT and cloud computing in healthcare has the potential to increase staff satisfaction, patient safety, and operational efficiency. The proliferation of IoT in healthcare also raises significant privacy and security concerns. The passage discusses prevalent threats and assault types, as well as industry- specific security frameworks designed to mitigate these risks. While established security models offer some level of protection, emerging trends and challenges could affect the future of IoT in healthcare.

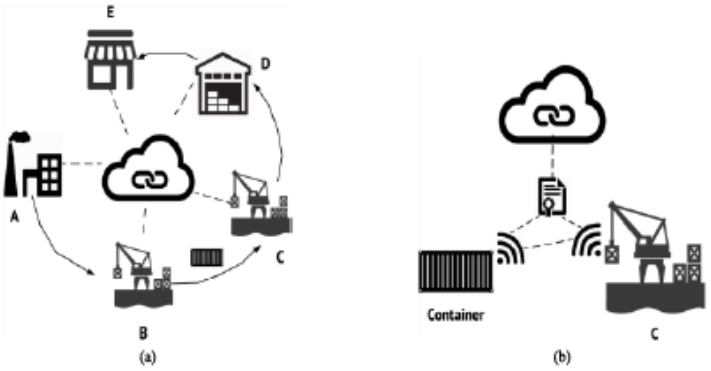


Figure 3: An asset tracking example using smart contracts and IoT.

2. Opening of the scheme proposed

Blockchain and IoT have enabled revolutionary healthcare solutions, particularly in secure data sharing and authentication. This integration is used to create a scalable authentication mechanism for Internet of Medical Things (IoMT) devices, which are essential to individualized health monitoring and smart healthcare. Blockchain technology's decentralization and immutability are used to ensure IoMT device authentication in this system. Traditional centralized authentication methods are vulnerable to cyberattacks and DDoS attacks, putting patient safety and healthcare data integrity at risk. In comparison, blockchain-based schemes are more secure. Smart contracts, self-executing contracts with coded terms, form the foundation of the proposed approach. Smart contracts on Ethereum can validate and authenticate IoMT devices without central authority. This feature boosts security and decreases counterfeit device entry into healthcare. IoMT devices are registered on the blockchain and identified via cryptography. This registration process verifies device validity with unique IDs and device-specific data. The blockchain's decentralization makes this data tamper-proof, giving healthcare providers and stakeholders a dependable source of truth. The suggested approach stresses safe firmware updates, which are essential for device integrity and security. Using blockchain technology, firmware updates may be securely disseminated and validated, preventing unauthorized changes or attacks. This function improves healthcare IoMT device safety and reliability. Healthcare privacy and confidentiality are important; hence the suggested scheme uses consortium blockchain architecture. Only authorized users can view and manage sensitive data using this design. This degree of privacy protects patient data and meets industry requirements. The proposed approach provides a secure, decentralized framework for healthcare IoMT device authentication, improving safety, reliability, and data integrity. Blockchain and smart contracts decrease security risks in centralized systems, making individualized health monitoring and intelligent healthcare safer.

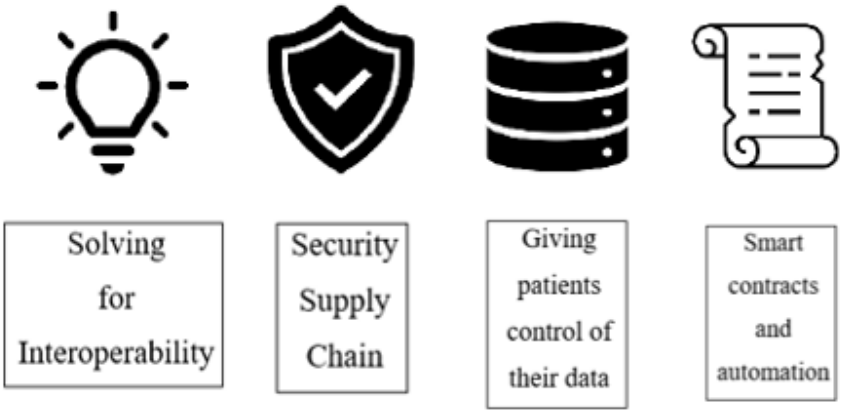


Figure 4: Empowering Healthcare Through Interoperability, Security, and Patient-Centric Data Solutions.

a. Implementation of the system

In healthcare, a comprehensive strategy is required to implement a system that integrates blockchain technology and the Internet of Things (IoT) to guarantee secure data exchange, patient data protection, and operational effectiveness. This process entails the development of decentralized architectures, the implementation of secure communication protocols, and the utilization of robust authentication mechanisms to safeguard confidential patient data while facilitating the exchange and availability of data.

i. Block chain Framework

The blockchain framework, which functions as a decentralized and immutable ledger system, is the foundation of the implementation. Block chain technology guarantees the security of data transmission and storage in the healthcare industry by generating a public and auditable ledger of every transaction. Key components for the implementation of a system encompass transaction validation across the Blockchain Network. A consensus mechanism, such as Proof of Work (PoW) or Proof of Stake (PoS), is employed to ensure the integrity of transactions. Consortium blockchains are frequently favored in the healthcare industry due to their combination of decentralized security and authorized-party access control. Smart contracts function as a mechanism to enforce regulations between parties automatically and without the need for intermediaries. In healthcare, they play a vital role in performing essential functions such as authenticating IoMT devices, facilitating automated processes like insurance claims and patient record sharing, and ensuring the security of data exchange.

The integration of IoT with block chain technology is of utmost importance in facilitating intelligent healthcare services and individualized health monitoring. IoT device connectivity is a critical factor in enabling the exchange of real-time data. To achieve this, wearables and sensors must seamlessly integrate with blockchain technology, establishing secure communication, to ensure encrypted data transfer is required during implementation.

5.1.2 Authentication and Authorization:

To assure the authenticity of IoMT devices, the scalable authentication scheme leverages the decentralized nature of block chain. This method employs Physical Unclonable Functions (PUF's) to verify devices and thwart counterfeiting. To uphold the integrity of the device, the implementation incorporates secure firmware updates.

5.1.3 Data Storage and Analysis

The integration of cloud computing and fog computing into the system enables efficient management of the substantial quantities of data produced by IoT devices. Considerations regarding implementation include Cloud storage solutions for healthcare data are provided by cloud platforms on a scalable basis. To safeguard sensitive information, implementation requires configuring secure data storage, encryption, and access controls.

5.1.4 Fog Computing

By bringing data processing closer to IoT devices, fog computing enables real- time analysis and reduces latency. This methodology proves advantageous in healthcare situations that demand prompt decision-making.

5.1.5 Compatibility and Security

The maintenance of security and adherence to regulatory requirements is an essential component of healthcare system implementation. The following are measures taken to address privacy and security concerns

5.1.6 Data Encryption

To safeguard patient information, data encryption is required both in transit and at rest. Utilizing robust encryption algorithms and key management practices are components of implementation.

5.1.7 Control of Access and Privacy:

Fine-grained permissions and role-based access control (RBAC) guarantee that access to sensitive data is restricted to authorized personnel exclusively. Privacy and anonymity features safeguard patient identities.

5.1.8 Adherence to Regulations

It is imperative to adhere to healthcare regulations, including but not limited to HIPAA and GDPR. It is imperative that system implementation includes compliance checks and guarantees accurate documentation of all activities pertaining to data.

5.2 Deployment Considerations for Blockchain and IoT in Healthcare

Implementing blockchain and IoT technologies in healthcare involves several key deployment considerations to ensure optimal functionality, security, and compliance. These considerations address both the technical and regulatory aspects of integrating these technologies within the healthcare ecosystem.

5.2.1 Security and Data Privacy

The decentralized nature of block chain technology enhances data security, but healthcare applications must ensure compliance with strict data privacy regulations, such as HIPAA (Health Insurance Portability and Accountability Act) in the United States and GDPR (General Data Protection Regulation) in Europe. Deployment must ensure patient data confidentiality, withes cure encryption protocols for data stored on the block chain and during transmission. IoT devices should be designed to mitigate vulnerabilities, with robust authentication and secure firmware updates.

5.2.2 Interoperability and Integration

Healthcare systems often comprise multiple platforms, making interoperability a critical consideration. Block chain solutions should support integration with existing electronic health record (EHR) systems, laboratory systems, and other healthcare applications. Standards like HL7FHIR (Health Level Seven Fast Healthcare Interoperability Resources) can guide interoperability to ensure seamless data exchange across different systems.

5.2.3 Scalability and Performance

Healthcare environments can generate vast amounts of data, requiring blockchain solutions to be scalable and responsive. Deployment should consider the network's scalability to accommodate increasing data volumes and the latency impact on healthcare operations. Hybrid or consortium block chains may offer better scalability and performance for healthcare applications compared to public block chains.

5.2.4 Governance and Accountability

Block chain deployment in healthcare requires clear governance structures. Decision- makers must establish rules for data access, user roles, and permissions, ensuring accountability while maintaining data integrity. A consortium blockchain with a defined governance model can help healthcare entities manage shared responsibility for the block chain's operation.

5.2.5 Cost and Infrastructure

Implementing block chain and IoT technologies incurs costs related to infrastructure, hardware, software, and maintenance. Healthcare providers must assess the financial implications of deployment, including initial setup and ongoing operational costs. Cloud computing and fog computing can provide flexible infrastructure solutions, but their use must comply with healthcare-specific regulations.

5.2.6 User Training and Adoption

Successful deployment of blockchain and IoT in healthcare requires buy-in from healthcare professionals and other stakeholders. Comprehensive training programs are necessary to ensure users understand the technology, its benefits, and how to use it effectively. User adoption is crucial for realizing the technology's potential in improving healthcare outcomes.

5.2.7 Regulatory Compliance and Legal Considerations

Healthcare is heavily regulated, and block chain deployment must align with legal and regulatory frameworks. Healthcare providers should ensure compliance with local and international regulations governing patient data, electronic records, and cyber security. Legal considerations also include data ownership, intellectual property rights, and liability issues related to data breaches. Deploying block chain and IoT in healthcare requires a holistic approach that addresses security, interoperability, scalability, governance, cost, user training, and regulatory compliance. By carefully considering these factors, healthcare organizations can leverage these technologies to improve data security, streamline operations, and enhance

patient care.

3. CONCLUSION

Blockchain and IoT enhanced healthcare, safety and efficiency. Healthcare providers, pharmaceutical companies, labs, and hospitals securely exchange medical data utilizing blockchain's decentralized and irreversible ledger. Data security reduces errors and tampering, improving patient data accuracy and healthcare decision-making. Blockchain can certify IoMT devices for smart healthcare and individualized health monitoring. Blockchain and smart contract-based scalable authentication are safer than centralized, cyberattack-prone techniques. Blockchain safeguards firmware upgrades, privacy, and anonymity against counterfeit devices. IoT's rapid expansion has led healthcare to use cloud and fog computing for data storage and analysis. These technologies improve patient safety, staff happiness, and operational efficiency. Healthcare IoT and cloud computing are supported by global-health policies that encourage secure data sharing. Despite advancements, healthcare IoT issues persist. Health apps are subject to attacks, making privacy and security vital. Reviews are needed to determine how well security mechanisms avoid these vulnerabilities. IoT in healthcare has immense potential, but it also brings unique issues that require creative solutions and strong security. IoT and blockchain provide safe data exchange, operational efficiency, and tailored health monitoring, transforming healthcare. These modern healthcare tools are beneficial, but patient data must remain secure. However, issues like the intricacy of blockchain integration and the cost of consensus mechanisms need to be resolved. In order to improve flexibility, future study can investigate the integration of AI for policy optimization and predictive analysis. Other important topics for additional research include lightweight consensus algorithms to lower latency and interoperability across various blockchain platforms.

REFERENCES

[1] R. Akkaoui, “Blockchain for the Management of Internet of Things Devices in the Medical Industry,” IEEE Transactions on Engineering Management, vol. 70, no. 8, pp. 2707–2718, Aug. 2023, doi:10.1109/tem.2021.3097117.

[2] H. N. Dai, Z. Zheng, and Y. Zhang, “Blockchain for Internet of Things: A Survey,” IEEE Internet of Things Journal, vol.6, no. 5, pp.8076–8094, Oct.2019, doi:10.1109/jiot.2019.2920987.

[3] K. Christidis and M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things,” IEEE Access, vol. 4, pp. 2292–2303, 2016, doi: 10.1109/access.2016.2566339.

[4] P. K. Maliketal., “Industrial Internet of Things and its Applications in Industry4.0: State of The Art,” Computer Communications, vol. 166, pp. 125–139, Jan. 2021, doi: 10.1016/j.comcom.2020.11.016.

[5] K. Christidis and M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things,” IEEE Access, vol. 4, pp. 2292–2303, 2016, doi: 10.1109/access.2016.2566339.

[6] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, “Smart Contract-Based Access Control for the Internet of Things,” IEEE Internet of Things Journal, vol. 6, no.2, pp.1594–1605, Apr.2019, doi:10.1109/jiot.2018.2847705.

[7] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, “Blockchain Technologies for the Internet of Things: Research Issues and Challenges,” IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2188–2204, Apr. 2019, doi:10.1109/jiot.2018.2882794.

[8] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, “Applications of Blockchains in the Internet of Things: A Comprehensive Survey,” IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1676–1717, 2019, doi:10.1109/comst.2018.2886932.

[9] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, “Smart Contract-Based Access Control for the Internet of Things,” IEEE Internet of Things Journal, vol.6, no.2, pp.1594–1605, Apr.2019, doi:10.1109/jiot.2018.2847705.

[10] M. Andonietal., “Blockchain technology in the energy sector: A systematic review of challenges and opportunities,” Renewable and Sustainable Energy Reviews, vol. 100, pp. 143–174, Feb. 2019, doi:10.1016/j.rser.2018.10.014.

[11] T. McGhin, K. K. R. Choo, C. Z. Liu, and D. He, “Blockchain in healthcare applications: Research challenges and opportunities,” Journal of Network and Computer Applications, vol. 135, pp. 62–75, Jun. 2019, doi: 10.1016/j.jnca.2019.02.027.

[12] P. Dutta, T. M. Choi, S. Somani, and R. Butala, “Blockchain technology in supply chain operations: Applications, challenges and research opportunities,” Transportation Research Part E: Logistics and Transportation Review, vol.142, p.102067, Oct.2020, doi:10.1016/j.tre.2020.102067.

[13] H. M. Hussien, S. M. Yasin, N. I. Udzir, M. I. H. Ninggal, and S. Salman, "Blockchain technology the healthcare industry: Trends and opportunities," Journal of Industrial Information Integration, vol.22, p.100217, Jun. 2021, doi: 10.1016/j.jii.2021.100217.

[14] S. Khezr, M. Moniruzzaman, A. Yassine, and R. Benlamri, "Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research," Applied Sciences, vol. 9, no. 9, p.1736, Apr. 2019, doi: 10.3390/app9091736.

[15] Vithya Ganesan, B. Rahul, V. Anjana Devi, Sri Anima Padmini Viriyala, Ramya Govindaraj, Subrata Chowdhury, Jerry Chun-Wei Lin, "Blockchain based Smart Supply chain and Transportation for Agri 4.0", pages 135-156, Science Direct, April 2024.

[16] Viswanathan Ramaswamy, Saikat Maity, N. Mohana Priya, Vithya Ganesan, Sri Anima Padmini, Subrata Chowdhury, Saurabh Adhikari, "Studies on Potential Conflicts of Network Densification in 6G", pp 231-241, Proceedings of Second International Conference on Intelligent System, Springer Link, April 2024.